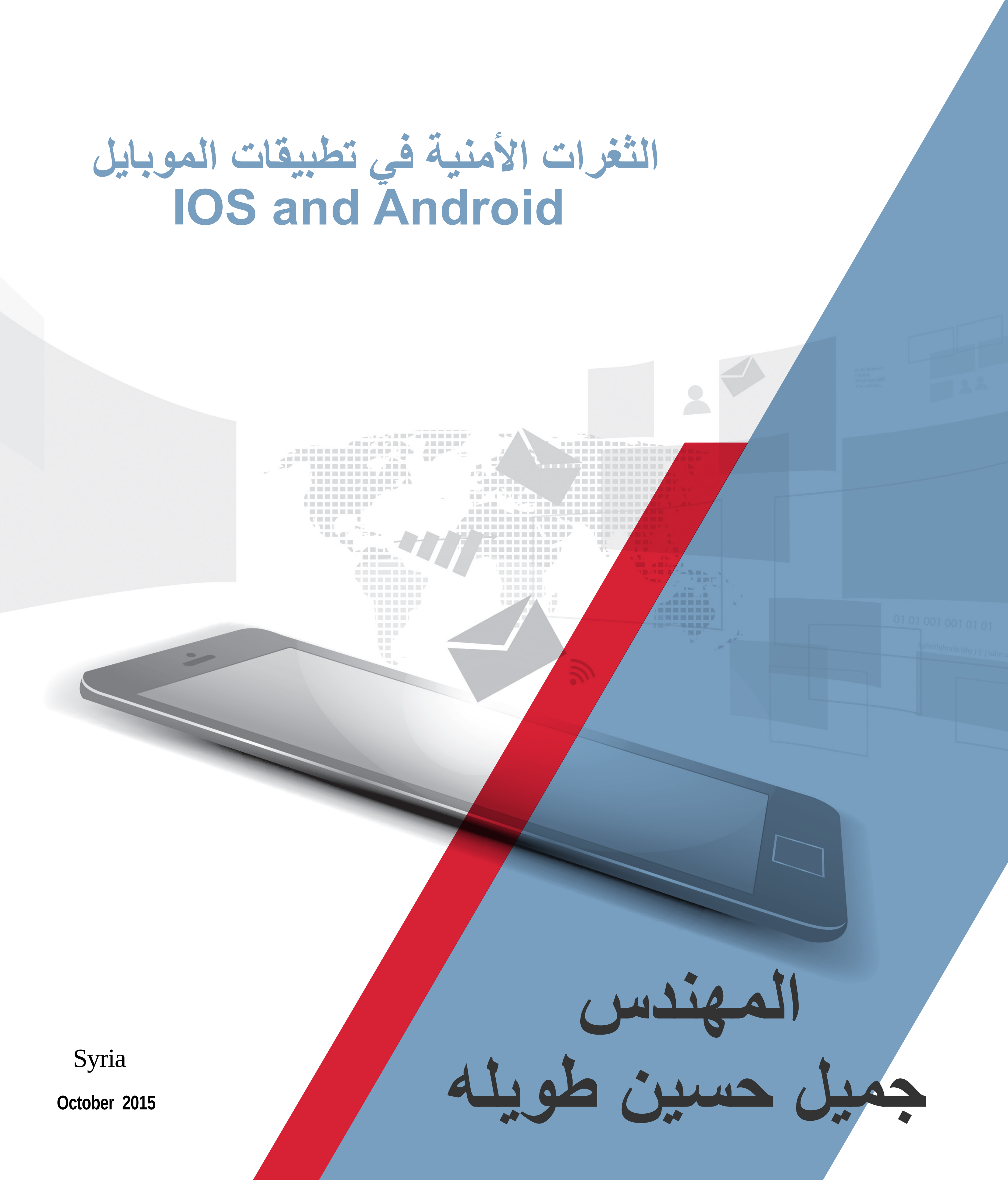
الثغرات الأمنية في تطبيقات الموبايل
IOS and Android



المهندس
جميل حسين طويله

Syria

October 2015

الثغرات الأمنية في تطبيقات الموبايل

IOS and Android

عن الكاتب:

جميل حسين طويله

مهندس اتصالات سوري

مختص في الشبكات اللاسلكية وأمن المعلومات واختبار الاختراق

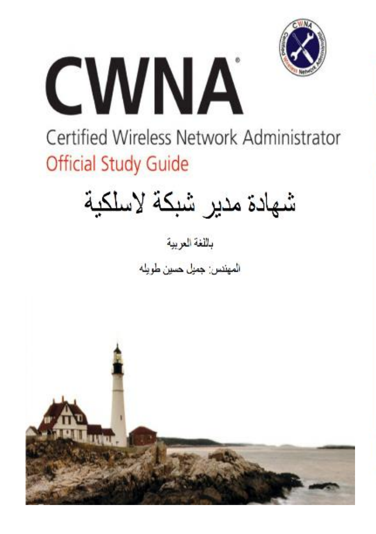
dolphin-syria@hotmail.com

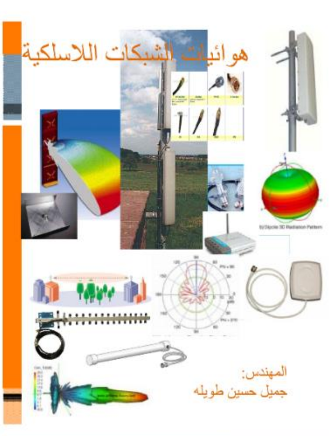
الإهداء:

إلى روح أبي وأمي رحمهما الله

إلى أرواح شهداء وطني سوريا

منشورات سابقة:





مدير شبكة لاسلكية

(3 أجزاء)

http://www.kutub.info/library/book/13857

http://www.kutub.info/library/book/13890

http://www.kutub.info/library/book/14144



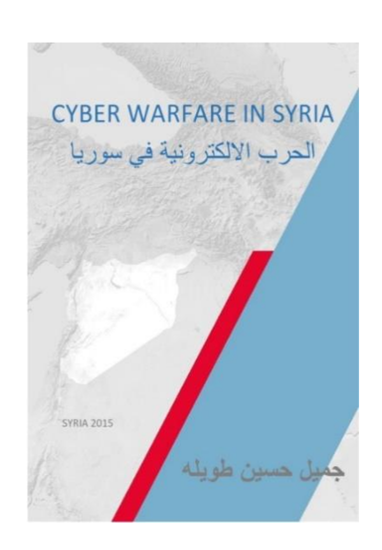
اختراق الشبكات اللاسلكية

http://www.kutub.info/library/book/15987



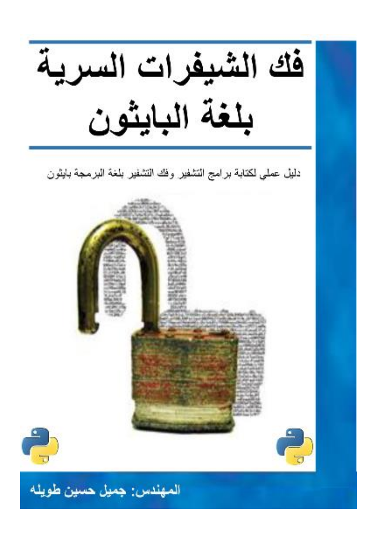
الحرب الالكترونية الأميركية في العراق

https://arabcyberwarrior.files.wordpress.com/2015/01/american-cyber-war-in-iraq.pdf



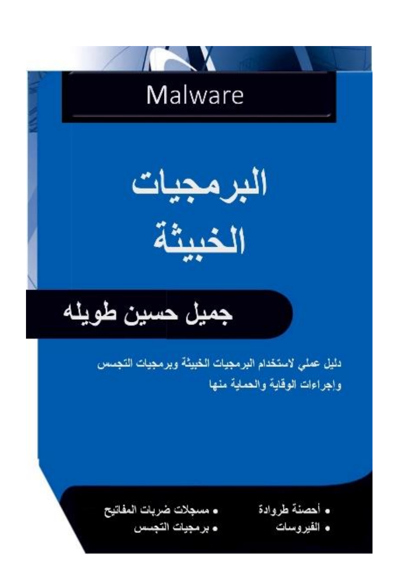
الحرب الالكترونية في سوريا

https://arabcyberwarrior.files.wordpress.com/2015/02/cyber-warfare-in-syria.pdf



فك الشيفرات السرية بلغة البايثون

https://arabcyberwarrior.files.wordpress.com/2015/03/arabic-hacking-secret-ciphers-with-python.pdf



البرمجيات الخبيثة

http://www.kutub.info/library/book/18976

أجهزة الموبايل أصبحت ذات أهمية كبيرة في الحياة الرقمية وإلى الآن مازالت معظم المنظمات والأشخاص لا يعيرون أي اهتمام لحماية أجهزة الموبايل من أجل الحفاظ على المعلومات والبيانات الموجودة في أجهزتهم بالرغم من انتشار عدد كبير جدد من التطبيقات التي يمكنها الوصول بسهولة إلى كامل بيانات الجهاز وسرقتها.

يوجد نظامين تشغيل أساسين تعمل بهمها أجهزة الموبايل:

- نظام الاندرويد الخاص بشركة غوغل Google's Android
- نظام IOS الخاص بشركة آبل Apple's IOS

المعلومات في هذا التقرير هي نتيجة لدراسات وتحليل قام بها الباحثون في شركة أمن المعلومات FireEye حيث قاموا بتحليل أكثر من 7 ملايين تطبيق موبايل لكلا نظامي التشغيل خلال الفترة بين شهر كانون الثاني إلى شهر تشرين الأول من عام 2014

التهديدات التي تواجه الأجهزة التي تعمل بنظام الأندرويد

برمجيات التجسس والاعلانات

5.61%

برمجيات التجسس و الإعلانات Adware يمكن أن تقوم بسرقة وتسريب المعلومات الشخصية للضحية أكثر برمجيات الإعلانات شهرة هو Bursty والذي يستخدم أكثر من 300,00 تطبيق والتي تحوي على نسبة 5.61% من أكثر 500 تطبيق يتم تحميله.

الثغرات

5 billion

أكثر من 5 بليون تحميل لتطبيقات اندرويد تحوي على ثغرات تسمح للمهاجم بالوصول و التحكم بجهاز الضحية من على بعد.

أكثر الثغرات خطورة هي:

JavaScript-Binding-Ove-HTTP (JBOH)

البرمجيات الخبيثة

يوجد الملايين من البرمجيات الخبيثة المصممة لتعمل ضد أجهزة الموبايل و هذه البرمجيات تزداد بشكل مستمر.

مثال على برمجية خبيثة تعمل على نظام الأندرويد هو تطبيق KorBanker الذي يقوم بسرقة بيانات تسجيل الدخول إلى الحسابات البنكية

التهديدات التي تواجه الأجهزة التي تعمل بنظام IOS

البرمجيات الخبيثة

المهاجمون يهتمون بهذه العامل بشكل كبير جداً.

ويقومون بنشر هذه البرمجيات للوصول للأجهزة التي لم يتم لها "jailbroken"

المهاجمون بدأو باستخدام تقنية اتصال enterprise/ad-hoc

من أجل توصيل البرمجيات الخبيثة إلى الأجهزة التي تعمل بنظام IOS والتي تكون non-jailbroken

من خلال اتصال USB موثوق به أو من خلال إرساله عبر اتصال لاسلكي

ENPUBLIC APPS

1400

هذه التطبيقات يمكنها تجاوز عملية التحقيق والمراجعة التي يقوم بها متجر تطبيقات آبل Apple's review من خلال سرقة عملية طبيعية تستخدم من أجل تنصيب تطبيقات للمستخدم.

العديد من تطبيقات EnPublic تحوي على واجهات مستخدم خطيرة تقوم باختراق الخصوصية وتؤدي لظهور العديد من الثغرات.

يوجد فقط 1,400 تطبيق EnPublic و هو عدد قليل ولكنه هذه التطبيقات ستكون الطريقة الأكثر استخدام من قبل المهاجمين في المستقبل.

الثغرات

UXSS

استعمال SSL/TLS وتقنيات التشفير الأخرى بشكل خاطىء أدى لوجود ثغرات في التطبيقات الأكثر شيوعاً.

الهجوم يتم غالباً من خلال استغلال ثغرات Universal Cross Site Scripting (UXSS)

المقدمة:

تطبيقات الموبايل أصبحت محور أساسي لكل النشاطات والأعمال وهي تسمح للشركات والأشخاص بخلق ومشاركة المعلومات بشكل سهل وسريع.

في عام 2014 كان معدل استخدام تطبيقات الموبايل هو 86% من وقت استخدام جهاز الموبايل وهذا المعدل كان قد ارتفع عن العام السابق بمقدار 6%

تطبيقات الموبايل الجيدة يمكن أن تساعد في كثير من الأمور أما التطبيقات السيئة يمكن أن تؤدي إلى ثغرات خطيرة وتفتح الباب أمام مخاطر أمنية كبيرة.

الهاكرز وجدوا في هذه التطبيقات طرق جديدة من أجل الوصول إلى أجهزة الموبايل في الوقت الذي كانت به طرق حماية أنظمة الموبايل في مراحلها الأولى.

معظم فرق الحماية لم يتمكنوا من مراقبة تطبيقات الموبايل التي تنتشر وتزداد بشكل يومي والتي كانت تحوي على ثغرات خطيرة تسمح للمهاجم بالوصول إلى كل بيانات جهاز الموبايل.

معظم مشاريع وشركات الحماية لم تكن تهتم كثيراً بحماية أجهزة الموبايل ولم يكن يوجد طريقة فعالة للتعامل مع الهجمات المتقدمة التي تستهدف أجهزة الموبايل.

تطبيقات الموبايل كانت تشكل خطر أمني كبير بسبب وجود عدد كبير من التطبيقات الخبيثة.

هذا التقرير يسلط الضوء على المخاطر التي تواجه كل من نظامي تشغيل أجهزة الموبايل Android and IOS من ثغرات وبرمجيات خبيثة بالإضافة إلى تطبيقات الموبايل الغير خبيثة والتي تحوي على ثغرات خطيرة بالإضافة إلى الخطوات التي يجب اتباعها من أجل حماية أجهزة الموبايل.

المخاطر التي تواجه نظام الاندرويد:

أجهزة الموبايل التي تعمل بنظام التشغيل اندرويد تقوم بجمع معلومات شخصية حساسة بالإضافة وتقوم تحديد مكان المستخدم كما تقوم بجمع معلومات عن الأسماء والأرقام والصور ومقاطع الفيديو ومعلومات الملكية الفردية وهذا يعتبر هدف مغري للمهاجم ليقوم بسرقة هذه المعلومات.

الباحثون في شركة أمن المعلومات FireEye قاموا بتحليل أكثر من 7 مليون تطبيق موبايل خلال عام 2014 وكانت النتائج كالتالي:

- وجود عدد كبير من التطبيقات الخبيثة التي تقوم بسرقة المعلومات.
- وجود تطبيقات غير خبيثة كتبت أكوادها بشكل غير أمن وغير محمي.
- وجود تطبيقات غير خبيثة تستخدم مكتبات غير محمية أو تحوي على إعلانات خبيثة.
- البرمجيات الخبيثة والإعلانات الخبيثة والتي تعتبر آمنة يمكنها أن تتجاوز فحص الحماية الخاص بمتجر غوغل بلاي Google Paly
- وجود تطبيقات تسمح للمهاجم بانتحال شخصية الضحية.
- وجود تطبيقات تعود بربح مالي للمهاجم من خلال رسوم المكالمات وخدمة الرسائل النصية.

البرمجيات الخبيثة لنظام الاندرويد:

Android malware

يوجد الملايين من البرمجيات الخبيثة الخاصة بأجهزة الموبايل وهي تزداد بشكل مستمر.

في نظام التشغيل اندرويد يمكن أن تبدو البرمجية الخبيثة على انها تطبيق سليم وحتى في بعض التطبيقات الموثوقة يوجد برمجيات إعلانات وتجسس "adware" لا يمكن التحكم بها وهي تقوم بجمع أكبر قدر ممكن من المعلومات عن المستخدم وعن الجهاز لتستخدم هذه المعلومات في خلق الإعلانات.

عدد البرمجيات الخبيثة الخاصة بنظام الاندرويد (باستثناء برمجيات التجسس والإعلانات) بلغ تقريباً 240,000 في عام 2013 و زاد هذا العدد ليصبح حوالي 390,000 في عام 2014

بلغ عدد البرمجيات الخبيثة المصممة من أجل سرقة المعلومات المتعلقة بالحسابات المالية حوالي 1300 في نهاية عام 2013

KORBANKER
تطبيق يسرق معلومات الحسابات البنكية

هو أفضل مثال على برمجية خبيثة مصممة لتعمل على نظام التشغيل الاندرويد.

وهي تقوم بمهاجمة العديد من التطبيقات البنكية في كوريا الجنوبية وهذه البرمجية تكون متخفية على شكل تطبيق مخزن غوغل بلاي.

التروجان (حصان طروادة) KorBanker Trojan يقوم بخداع المستخدم من أجل الحصول على صلاحيات المدير (الأدمن) في الجهاز.

بعد أن يقوم المستخدم بتنصيب KorBanker يقوم هذا التطبيق الخبيث باستخدام واجهة تسجيل دخول مزورة fake login interface تشابه واجهة التطبيق البنكي الذي يستخدمه المستخدم.

العديد من الضحايا وقعوا في هذا الفخ وقاموا بكتابة معلومات تسجيل الدخول لحساباتهم البنكية في هذه الواجهة المزورة حيث يتم إرسال معلومات تسجيل الدخول إلى سيرفرات المهاجم الموجودة في هونغ كونغ.

:BURSTLY

بروستلي وهي شركة فرعية لشركة آبل Apple وهي متخصصة في تحليل واختبار تطبيقات المحمول وتقوم بعمل مكتبات الإعلانات ad library لدمجها مع تطبيقات نظامي التشغيل Android and IOS

أحد زبائن هذه الشركة هي شركة Rovio التي قامت بصناعة لعبة Angry Birds الشهيرة.

شركة بروستلي تقوم بجمع معلومات عن المستخدم مثل:

- العمر
- عدد الأولاد
- التحصيل العلمي
- الديانة
- الجنس
- الطول
- الدخل الشهري
- اهتمامات المستخدم
- الموقع
- الحالة الاجتماعية
- التوجه الجنسي
- الانتماء السياسي
- ZIP code

شركة بروستلي تقوم بجمع هذه المعلومات طول فترة حياة جهاز المستخدم وتقوم بخلق ملفات تحوي على هذه التفاصيل وهذه الملفات تسمح للشركة ببيع إعلانات موجهة بشكل أكبر والتي يمكن أن تقنع المستخدم بشراء المنتج أكثر بخمس مرات من الإعلانات الغير موجهة.

أكثر من 300,000 تطبيق تستخدم مكتبات شركة بروستلي وهذه التطبيقات تحوي على 5.61% من أكثر 500 تطبيق يتم تحميله حول العالم.

تطبيقات الاندرويد التي تحوي على ثغرات:

أكثر من 5 بليون تحميل لتطبيقات اندرويد تحوي على ثغرات تسمح للمهاجم التحكم بجهاز الضحية من على بعد.

نظام التشغيل اندرويد الخاص بشركة غوغل يحوي على العديد من الثغرات والتي يمكن للمهاجم استغلالها

وأخطر هذه الثغرات هي ثغرة JavaScript-Binding-Over-HTTP(JBOH)

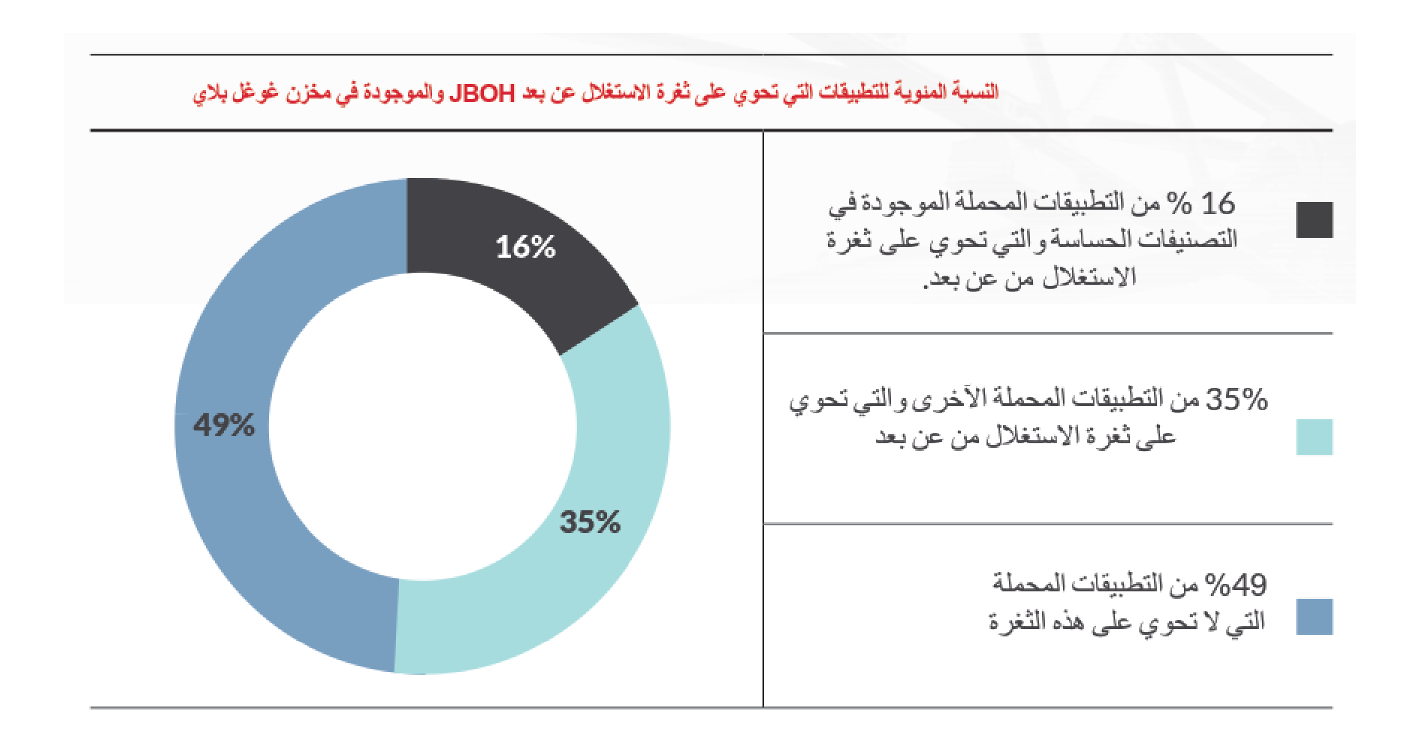
هذه الثغرة تستخدم طريقة شائعة من أجل تحميل محتوى الويب إلى تطبيق الاندرويد وهي طريقة غير آمنة

عندما يقوم التطبيق باستخدام هذه الطريقة ويقوم بتحميل محتوى من متصفح الويب في WebView عبر برتوكول HTTP و يفتح باب للمهاجم من أجل أن يقوم بتنفيذ كود خبيث من عن بعد

(WebView هي طريقة عرض محتوى الويب في تطبيقات الاندرويد)

أي أن المهاجم يستطيع أن يسرق اتصال HTTP من أجل أن يقوم بحقن المحتوى الخبيث والروابط في الكود الخاص ب WebView ويحصل على تحكم كامل بالتطبيق الذي يعمل في الجهاز.

الباحثون في شركة أمن المعلومات FireEye قاموا بتحليل التطبيقات الأكثر تحميلاً (التي تم تحميلها أكثر من 50,000 مرة) من أجل تحديد نسبة تعرضها لثغرة وهجوم JBOH وكانت نسبة الإصابة بهذه الثغرة هي 31% وحوالي 18% منها تقع في تصنيفات تحوي على معلومات حساسة مثل التطبيقات المالية و الطبية وتطبيقات التسوق والاتصالات.



برمجيات التجسس والاعلانات الخاصة بنظام الاندرويد:

Android adware

مكتبات الإعلانات يمكن أن تقوم بتسريب المعلومات الشخصية عبر الشبكة وفي بعض الحالات تكون هذه المعلومات على شكل نص صريح ويمكن لأي شخص يراقب حركة البيانات في الشبكة رؤية هذه المعلومات.

برمجيات الإعلانات والتجسس Adware هي عبارة عن برمجيات تقوم بعرض الإعلانات من أجل الحصول على المال وهذا النوع من البرمجيات ليس مؤذي أو خطير بحد ذاته.

هذه البرمجيات وبعد تنصيبها على جهاز الموبايل تقوم بجمع المعلومات الشخصية من الجهاز مثل اسم المستخدم وتاريخ ميلاده وموقعه الجغرافي ورقم الجهاز التسلسلي والأسماء والصفحات والعلامات المحفوظة في متصفح الويب وهذه المعلومات تجمع بدون موافقة أو معرفة المستخدم.

برمجيات الإعلانات Adware هي خيار مرغوب جداً لناشري التطبيقات وقد زاد عددها من 300,000 تطبيق في عام 2013 إلى 410,000 تطبيق في منتصف عام 2014

تصنيف التطبيقات التي تحوي على برمجيات الإعلانات هي:

- التطبيقات ذات الطابع الشخصي
- تطبيقات التسلية والألعاب
- تطبيقات أسلوب الحياة Lifestyle apps

تطبيقات الألعاب والاتصالات غالباً تحوي على برمجيات للإعلانات والتي تقوم بجمع معلومات عن اهتمامات المستخدم لتتمكن من صناعة إعلانات موجهة.

المخاطر التي تواجه نظام IOS:

البرمجيات الخبيثة الخاصة بنظام تشغيل أجهزة الموبايل IOS مازالت قليلة ونادرة نتيجة عملية التنقيح والمراجعة الصارمة في مخزن آبل Apple's app store

ولكن حديثاً تم الكشف عن قناة لتوزيع البرمجيات الخبيثة التي يمكنها تجاوز أو تخطي عملية التنقيح والمراجعة بشكل كامل.

تطبيقات المشاريع Enterprise apps لا تخضع لعملية التنقيح والمراجعة المعيارية لتطبيقات آبل وهذا يعرض المستخدمين لمخاطر كبيرة.

المخاطر التي تواجه نظام IOS يمكن تصنيفها كالتالي:

- الثغرات وتسريب المعلومات وخاصة من التطبيقات التي تعمل في الخلفية.
- التطبيقات العامة تنتشر عبر enterprise provisioning وتعرف باسم EnPublic
- البرمجيات الخبيثة.

ثغرات نظام IOS نادرة ولكنها خطيرة جداً إن وجدت:

مثلاً التطبيقات التي تستخدم enterprise/ad-hoc provisioning وحتى بعض التطبيقات ذات السلوك العدواني في مخزن تطبيقات آبل يمكن أن تستغل العديد من ثغرات نظام IOS

وبالتحديد الاستخدام الخاطئ ل SSL/TLS (Secure Socket Layer/ Transport Level Security) برتوكولات التشفير والحماية وتقنيات التشفير الأخرى يؤدي لظهور ثغرات في التطبيقات المشهورة.

المهاجم يستطيع أيضاً استغلال ثغرة Universal Cross-Site Scripting (UXSS)

المهاجم يستخدم التطبيقات الغير موثقة (التي يتم رفضها من خلال عملية التنقيح والمراجعة الخاصة بشركة آبل) من أجل القيام بهجوم قوي.





في عام 2014 كان لهجوم Masque تأثير كبير على آمن وحماية نظام IOS

المهاجمون قاموا بتقليد واجهة تسجيل الدخول لتطبيقات أصلية من أجل القيام بسرقة معلومات تسجيل الدخول الخاصة بالضحايا وتم التأكد من ذلك من خلال عدة ايميلات وتطبيقات بنكية حيث تقوم البرمجية الخبيثة باستخدام واجهة مستخدم مماثلة لواجهة التطبيق الأصلي.

الواجهة المزورة تخدع المستخدم الذي يقوم بكتابة معلومات تسجيل الدخول ومن ثم ترسل هذه المعلومات إلى السيرفر الخاص بالمهاجم.

من خلال الدراسة والتحليل تم اكتشاف أن البيانات المحلية المخبئة local data caches الموجودة في مجلد التطبيق الأصلي تبقى في المجلد المحلي للبرمجية الخبيثة بعد أن يتم استبدال التطبيق الأصلي.

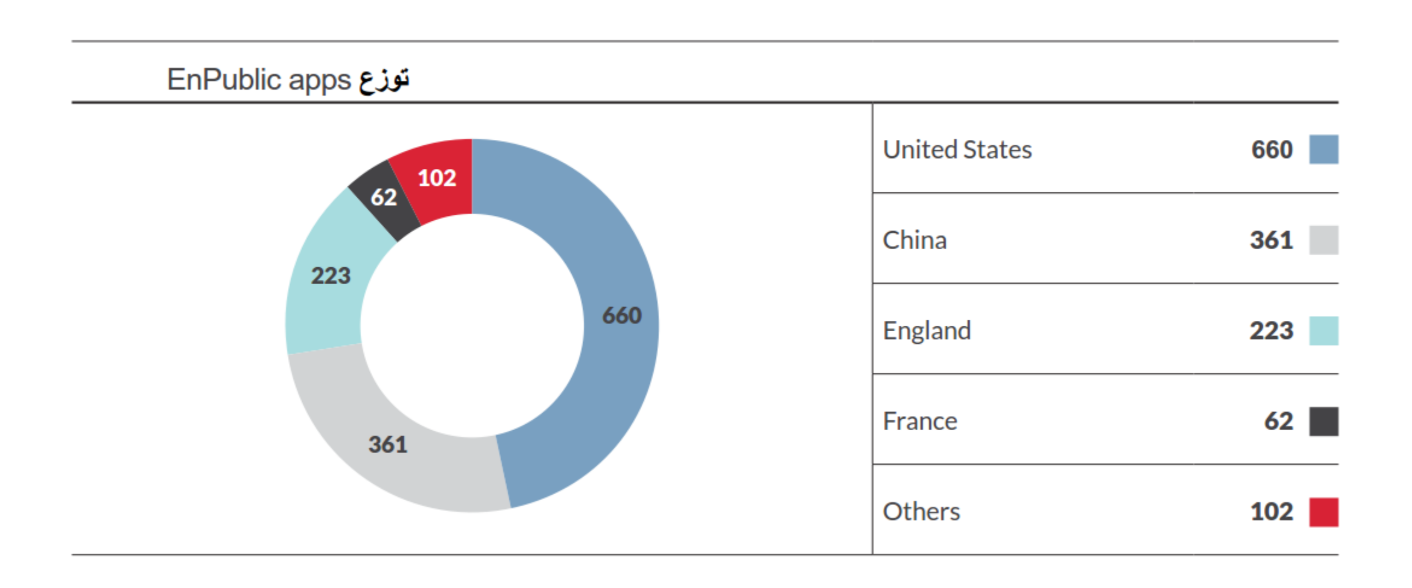
البرمجية الخبيثة تقوم بسرقة هذه المعلومات الحساسة وتم التأكد من هذا الهجوم من خلال تطبيق الايميل حيث قامت البرمجية الخبيثة بسرقة ملفات local caches للإيميلات المهمة ورفعها إلى السيرفر البعيد الخاص بالمهاجم.

تقنية إدارة جهاز الموبايل (Mobile device management MDM لا تستطيع التمييز بين تطبيق البرمجية الخبيثة وبين التطبيق الأصلي لأن لكلا التطبيقين نفس حزمة التعريف bundle identifier

المهاجم يستطيع استخدام تطبيقات IOS الغير موثقة (التي يتم رفضها من خلال عملية التنقيح في متجر تطبيقات آبل) من أجل القيام بهجوم قوي، المهاجم يستطيع رؤية ومراقبة كل أفعال المستخدم كما يمكنه محاكاة وتقليد واجهة iCloud's interface (هجوم التصيد من خلال استخدام واجهة مزورة) من أجل سرقة كلمة السر ومُعرف Apple ID الخاص بالمستخدم.

المهاجم يستطيع أيضاً استخدام هجوم Masque attack من أجل الحصول على صلاحيات الروت root (صلاحيات المدير) من خلال مهاجمة ثغرات IOS المعروفة مثل الثغرة التي استخدمها فريق Pangu team من أجل القيام بعملية jailbreak لأجهزة التي تعمل بنظم IOS

أكثر من 80% من تطبيقات EnPulic تستخدم واجهات برمجية خاصة private API محظورة من قبل آبل



تجاوز عملية التنقيح والمراجعة باستخدام تطبيقات EnPublic:

خلال عملية التحليل تم اكتشاف قناة جديدة لتسليم البرمجيات الخبيثة الخاصة بنظام IOS والتي يتم من خلالها تجاوز عملية التنقيح والمراجعة التي يقوم بها متجر تطبيقات آبل

bypass Apple App Store review process

يوجد أكثر من 1,400 تطبيق خاص بنظام IOS متوفرة عبر الانترنت وبشكل مجاني و موقعه بشهادات enterprise certificates هذه التطبيقات تسمى EnPublic apps

وهي مصممة بالأصل من أجل بناء تطبيقات منزلية ولكن مطورو هذا البرنامج Enterprise Program اساءوا توزيع تطبيقات IOS الغير خاضعة لعملية التنقيح والمراجعة وبالنتيجة تم نشر هذه التطبيقات بدون أي حماية أو تحكم بالخصوصية.

أكثر من 80% من تطبيقات EnPublic apps تستخدم واجهات برمجة تطبيقات خاصة private APIs محظورة من قبل آبل

API (Application Program Interface)

تطبيقات EnPublic يمكنها استخدام واجهات برمجية خاصة private APIs داخل نظام IOS وتقوم بتحميل واجهة مستخدم مماثلة لتطبيقات آبل الأصلية.

المهاجم يقوم بإرسال رسالة نصية أو رسالة عبر الايميل تحوي على رابط من أجل تحميل تطبيق EnPublic

تطبيقات EnPublic تمثل خطر أقل بالمقارنة مع البرمجيات الخبيثة الخاصة بنظام الاندرويد ولكن هذه الطريقة في الهجوم والاستغلال من المحتمل أن تنمو وتزداد.

البرمجيات الخبيثة الجديدة لنظام IOS:

تقريباً معظم البرمجيات الخبيثة التي تم اكتشافها تعمل فقط ضد الأجهزة التي تم لها عملية jailbroken ولكن هذا تغير في خريف 2014 عندما تم اكتشاف نوعين من البرمجيات الخبيثة الخاصة بنظام IOS

وهما WireLurker and Pawn Storm الذين اساءا استخدام enterprise and ad-hoc provisioning من أجل تنصيب برمجيات خبيثة على الأجهزة التي تكون non-jailbroken

WireLurker يستخدم اتصال USB موثوق به من أجل تنصيب البرمجية الخبيثة على الأجهزة التي تعمل بنظام IOS وفي كلا الحالتين jailbroken and non-jailbroken وهو يستخدم enterprise provisioning من أجل تنصيب البرمجية الخبيثة.

وبشكل مختلف عن WireLurker المصمم ليقوم بأخذ المال من الضحايا فإن Pawn Storm هو برمجية خبيثة تستخدم للتجسس على الأجهزة التي تكون non-jailbroken وهي تقوم بجمع البيانات والمعلومات وتقوم بإلتقاط صور للشاشة وترسلهم إلى سيرفر التحكم والقيادة Command and Control (C2) server الخاص بالمهاجم.

الخلاصة:

أجهزة الموبايل هي الخيار المفضل لمعظم الناس حول العالم.

مبيعات أجهزة الحاسوب تناقصت بسبب اختيار الناس لأجهزة الموبايل لأنها أخف واسهل استخداماً

نحن نمضي الكثير من الوقت في استخدام جهاز الموبايل ومعظم هذا الوقت يكون لاستخدام التطبيقات والعديد من الأشخاص يستخدمون هذه التطبيقات من أجل العمل والتسوق والعمليات البنكية والمصرفية والعديد من الأمور الأخرى.

بالنسبة لمعظم الناس فإن جهاز الموبايل أصبح أكثر أداة مهمة في حياتهم لأنه يحوي على قوائم الأسماء و الايميلات والصور ومقاطع الفيديو والكثير من المعلومات المهمة الأخرى.

وحتى الآن أجهزة الموبايل تعاني من ضعف في الحماية وهي غير قادرة على المحافظة على المعلومات والبيانات المهمة بشكل آمن ومحمي.

أجهزة الموبايل تواجه العديد من التهديدات الأمنية الرقمية بسبب المخاطر التي تتعرض لها من قبل مخازن التطبيقات ومطوري التطبيقات.

التطبيقات التي نقوم بتحميلها يمكن أن تقوم بسرقة وكشف كل المعلومات والبيانات الموجودة في جهاز الموبايل

التطبيقات الخبيثة تستطيع سرقة تفاصيل الحسابات البنكية ونسخ الايميلات وجمع المعلومات الخاصة باتصالات VPN (Virtual Private Network) المحمية.

برمجيات الإعلانات Adware تقوم بجمع المعلومات الشخصية ومعلومات عن التطبيقات المستخدمة بالإضافة إلى معلومات تحديد الموقع GPS بدون علم أو موافقة المستخدم.

معظم متاجر التطبيقات تعمل من أجل كشف ورفض التطبيقات المؤذية ولكن المهاجمون يقومون بخلق تطبيقات تحوي على ميزات جديدة غير متوفرة في التطبيقات العادية ويقومن بإخفاء التطبيقات الخبيثة في داخلها.

يجب أن تفهم جيداً المخاطر الأمنية لتطبيقات الموبايل وتقوم بمراقبة سلوك هذه التطبيقات بشكل مستمر.